Hrebeniuk, A.M., Rybalchenko, L.V., & Prokopov, S.O. (2022). Monitoring of cyber incidents of cloud services and protection of digital communication channels. *The First Special Humanitarian Issue of Ukrainian Scientists. European Scientific e-Journal, 3* (18), 40-53. Ostrava: Tuculart Edition. (in Ukrainian)
Гребенюк, А.М., Рибальченко, Л.В. та Прокопов, С.О. (2022). Моніторинг кіберінциндентів хмарних сервісів та захист цифрових каналів зв'язку. *The First Special Humanitarian Issue of Ukrainian Scientists. European Scientific e-Journal, 3* (18), 40-53. Ostrava: Tuculart Edition.

DOI: 10.47451/inn2022-04-01

The paper will be published in Crossref, ICI Copernicus, J-Gate, ISI, Academic Resource Index ResearchBib, Internet Archive, Google Scholar, eLibrary, Ukrainian National Library databases.



Andrii M. Hrebeniuk, Candidate of Technical Sciences, Associate Professor of the Department of Economic and Information Security, Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine. ORCID: 0000-0002-6529-683X.
Lyudmila V. Rybalchenko, Candidate of Economic Sciences, Associate Professor of the Department of Economic and Information Security, Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine. ORCID: 0000-0003-0413-8296.
Serhii O. Prokopov, Senior teacher, Department of Economic and Information Security Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine.
ORCID: 0000-0002-7247-5780.

Monitoring of cyber incidents of cloud services and protection of digital communication channels

Abstract: This article is dedicated to cloud services and modern possibilities of protection of digital communication channels. Today, usage of cloud technologies is steadily increasing both in business and in everyday life. Saving and processing of large amounts of information in a virtual environment is accomplished through the hardware and software, as well as communication channels of the provider. Fast access and reliable protection of personal data is an important part of the basic requirements of work with modern smart technologies. The purpose of the research is the analysis and monitoring of security in the cloud services. In the course of the research to achieve the set goal were used the following methods: methods of comparison, statistical and graphical analysis. In the article were used the previous scientific research works of various authors, as well as the periodic ranking surveys of popular world economic agencies and forums. The authors concluded that the most effective is the passwordless login technology, which supports authentication based on certificates, ensures secure storage and management of certificates, which are linked to the user and a specific device.

Key words: cloud technology, personal data protection, hybrid cloud monitoring, fraudulent records, cyber fraud, confidential information.



Андрій Миколайович Гребенюк, кандидат технічних наук, доцент, Кафедра економічної та інформаційної безпеки, Дніпропетровський державний університет внутрішніх справ, Дніпро, Україна. ORCID: 0000-0002-6529-683X.
Людмила Володимирівна Рибальченко, кандидат економічних наук, доцент, Кафедра економічної та інформаційної безпеки, Дніпропетровський державний університет нутрішніх справ, Дніпро, Україна. ORCID: 0000-0003-0413-8296.

Сергій Олександрович Прокопов, ст. викладач, Кафедра економічної та інформаційної безпекиб Дніпропетровський державний університет внутрішніх справ, Дніпро, Україна. ORCID: 0000-0002-7247-5780.

Моніторинг кіберінциндентів хмарних сервісів та захист цифрових каналів зв'язку

Анотація: Стаття присвячена хмарним сервісам та сучасним можливостям захисту цифрових каналів зв'язку. Застосування хмарних технології на сьогоднішній день постійно зростає як у бізнесі так і у повсякденному житті. Збереження та обробка великих обсягів інформації у віртуальному середовищі створюється із застосуванням апаратних засобів, програмного забезпечення та каналів зв'язку провайдера. Швидкий доступ та надійний захист персональних даних є важливою складовою щодо основних вимог роботи із сучасними хмарними технологіями. Метою дослідження є аналіз та моніторинг забезпечення безпеки у хмарних сервісах. У ході дослідження для досягнення поставленої мети застосовувались методи порівняння, статистичного та графічного аналізу. У дослідженні застосовано попередні наукові праці авторів, періодичні рейтингові дослідження популярних світових економічних агенцій та форумів. Автори дійшли висновку, що технологія безпарольного входу, яка підтримує автентифікацію на основі сертифікатів, забезпечує безпечне зберігання та керування сертифікатами, які прив'язані до користувача та конкретного пристрою, є найбільш ефективною.

Ключові слова: хмарні технології, захист персональних даних, гібридний хмарний моніторинг, шахрайські записи, кібершахрайство, конфіденційна інформація.



Вступ

В теперішній час, з приходом пандемії та в контексті бойових дій, в нашій країні актуальним стало застосування хмарних технологій для спільного використання і збереження інформації.

Щорічне зростання діджиталізації у світі та необхідність роботи із інноваційними технологіями, призводить до всебічного прояву економічної злочинності, актуальність і необхідність якої є важливою для ґрунтовних наукових досліджень щодо забезпечення надійного захисту персональних даних у хмарних сервісах та зменшення рівня постраждалих від різноманітних економічних злочинів. Зростання кіберзлочинності, шахрайства та інших економічних злочинів, пов'язано з ризиками та загрозами в усіх сферах життєдіяльності особистості.

Метою даного дослідження є аналіз та моніторинг забезпечення безпеки у хмарних сервісах. Для досягнення поставленої мети було проаналізовано рейтинги найпопулярніших послуг хмарного хостингу, виявлено облікові записи із найбільшою кількістю економічних злочинів, що призвели до фінансових втрат майже третину компаній та організацій в Україні та світі.

Зростання економічних злочинів, шахрайства та кібератак відбуваються через стрімкий розвиток новітніх технологій та цифрової економіки, в яку поглинули усі сфери діяльності в усьому світі.

Застосування методів порівняння, статистичного та графічного аналізу дало можливість дослідити праці вітчизняних (*Rybalchenko et al., 2021a; Rybalchenko et al., 2021b; Rubalchenko & Ryzhkov, 2019; Rubalchenko & Kosychenko, 2019*) та зарубіжних науковців (*Less than 20% of IT pros have complete access to critical data in public clouds, 2019*; *How do you protect digital channels from cyber threats?, 2018*; *For some cloud services more than 75% of accounts are utilized by hackers, 2018*; *Національний індекс кібербезпеки, 2020*; *Global Cybersecurity Outlook 2022*), світові рейтингові агенції для впровадження сучасних технологій щодо забезпечення постійного захисту та моніторингу задля протидії економічним злочинам, шахрайству та кіберзлочинності.

Основна частина

Складність хмар зростає з кожним роком, а гібридна хмара стала новою інфраструктурою. Хоча віртуальні машини залишаються найпоширенішим середовищем хмарних обчислень (83%), контейнери (37%), без серверів (28%) та сервісні сітки (21%) набирають популярність. Гібридні та багатохмарні підходи зараз складають більше третини усіх конфігурацій (77%).

Із зростанням складності хмарної інфраструктури, безпека стає спільною відповідальністю DevOps (development & operations - це методологія автоматизації технологічних процесів збору та впровадження програмного забезпечення). Менше половини організацій (45%) зараз мають спеціальну групу безпеки, відповідальну за хмару, а 35% усіх організацій зараз використовують або команду DevOps, або спеціальну команду DevSecOps (розробка, експлуатація та безпека) для безпеки (*Рис. 1*).

Незважаючи на деякі проблеми безпеки, більшість (57%) безсерверних користувачів наразі використовують його як у виробництві, так і в процесі розробки. Більшість, які зараз використовують безсерверні програми, мають високий ступінь впевненості у його безпеці, тоді як третина (32%) висловлюють невпевненість у безпеці свого середовища. (*Рис. 2*)

Склад гібридної хмари спонукає команди DevSecOps шукати більше інструментів для захисту своїх розподілених середовищ. Понад 75% очікують збільшення кількості інструментів, що використовуються, протягом наступних дванадцяти місяців, при цьому ніхто не очікує відмови від використання будь-яких інструментів. Третина організацій, що звітують, використовують більше п'яти інструментів для безпеки хмар. Поширення хмарних засобів безпеки залишає підприємство вразливим, що вказує на необхідність інтелектуальної автоматизації політики. Більше половини (60%) організацій покладаються на ручні конфігурації політик безпеки своїх програм, тоді як майже всі організації (90%) покладаються на кількох осіб для налаштування та встановлення правил політики.

Ця відсутність наочності може призвести до поганої продуктивності додатків, втрати даних клієнтів та невизначених загроз безпеці, що все може мати серйозні наслідки для загального успіху бізнесу в організації. Громадський та гібридний хмарний моніторинг має потужності щодо відстеження традиційних центрів обробки даних.

Опитування зосереджувалося на проблемах, з якими стикається моніторинг публічних та приватних хмар, а також локальних центрів обробки даних. Дані, виявлені

ІТ-спеціалістами, показали, що хмарні провайдери не забезпечують необхідного рівня видимості:

- середовища загальнодоступних хмар важко контролювати: менше 20% ІТ-фахівців повідомили, що вони мали повний, своєчасний доступ до пакетів даних у загальнодоступних хмарах. У приватних хмарах ситуація краща: 55% повідомляють про належний доступ. У локальних центрах обробки даних 82% мають необхідну видимість;
- видимість на рівні пакетів має вирішальне значення для моніторингу: 86% респондентів зазначили, що видимість важлива для моніторингу продуктивності мережі та додатків, а 93% заявили, що вона важлива для безпеки (*Рис. 3*).

Рішення для видимості покращують моніторинг, управління продуктивністю мережі та безпеку. Майже всі респонденти (99%) виявили прямий зв'язок між загальною видимістю мережі та цінністю бізнесу. Пропоновано три найкращі переваги видимості:

1) моніторинг та забезпечення продуктивності програми (60%);
2) увімкнення ідентифікації загрози (59%);
3) визначення «показників компромісу» безпеки (57%).

Опитування також показало, що видимість має вирішальне значення для моніторингу продуктивності хмар, а також перевірки продуктивності додатків до розгортання хмари. Передбачення продуктивності – ключовий виклик, 87% користувачів хмари важко передбачити продуктивність додатків у хмарі (*Less than 20% of IT pros have complete access to critical data in public clouds, 2019*).

Зараз організації активно об'єднуються, що дозволяє їм зберігати великі обсяги даних і додатків з більш високою безвідмовною роботою та із зниженням витрат.

Однією з найбільш помітних проблем є управління особистими даними та авторизація. З початку хмарних обчислень методи авторизації в хмарі перетворилися на нові моделі, які визнають безліч різноманітних послуг, які тепер об'єднуються, щоб сформувати мережу компанії.

Ці підходи враховують зростаючу кількість сліпих місць безпеки та слабких місць у хмарному середовищі. Замість того, щоб з'єднуватись дротом у межах корпоративної мережі, більшість цих нових послуг відкриті для Інтернету, розширюючи поверхню атаки інфраструктури компаній.

Наведемо п'ять ключових подій, які слід розглянути для управління авторизацією в хмарі.

Централізоване управління та розподілені послуги

У традиційному локальному середовищі всіх користувачів зазвичай обслуговував єдиний сервер, який обслуговував би кожну програму, незалежно від того, надавати чи забороняти доступ. У хмарному середовищі кожна служба має свій власний набір дозволів та ідентифікаційних даних, а також власний механізм авторизації та автентифікації для їх підтримки та застосування. Це значно ускладнює налаштування та відкриває низку проблем помилок конфігурації, що призводить до хмарних атак.

Послуги з авторизації

Для того, щоб керувати користувачами на єдиній платформі, використовується одна зовнішня служба авторизації. Ви надаєте облікові дані служби авторизації обліковому запису, який може створювати тимчасові ролі або керувати вашими обліковими записами в одному хмарному сервісі, яким ви користуєтесь. Завдяки цьому користувачів можна визначити на одній платформі, але постачальнику ідентифікаційних даних потрібно довіряти, щоб він не виконував шкідливих дій, а коли це станеться, може бути важче відстежити, звідки ці дії виникли.

Методи хмарної авторизації різні, включаючи MAC – де кожен додаток володіє індивідуальними дозволами доступу, DAC – де кожен додаток запитує дозволи від зовнішньої програми дозволів, RBAC – де служба авторизації володіє ролями з різними привілеями у хмарній службі та ABAC – де доступ базується на атрибутах та політиці запиту.

Статистичний аналіз кіберінциндентів хмарних сервісів

Для деяких хмарних сервісів більше 75% облікових записів використовуються хакерами. Дослідники виявили, що 21,57% відсотків облікових записів, що походять із діапазонів IP-адрес хмарного сервісу, є шахрайськими. Шкідливі облікові записи у вісім разів частіше виникають через хмарні сервіси, ніж звичайні користувачі. Насправді, деякі хмарні служби та центри обробки даних можуть мати більше 75% шахрайських облікових записів (*Рис. 4*).

Звіт щодо індексу шахрайства DataVisor за 2 квартал 2021 року – це щоквартальна оцінка типів та методів шахрайства в Інтернеті на соціальних платформах та фінансових службах. Поточний звіт використовує інформацію, зібрану DataVisor у період з квітня по червень 2020 року, аналізуючи 1,1 мільярда активних облікових записів користувачів, 1,5 млн. доменів електронної пошти, 231000 типів пристроїв та 562 провайдерів хмарного хостингу та центрів обробки даних, серед інших показників.

Добре продумана та керована присутність у соціальних мережах є обов'язковою умовою для більшості компаній та їхньої робочої сили, але надто мало з них замислюються про потенційні наслідки атаки, спрямованої на неї.

Соціальні медіа все частіше сприймаються як поле битви, забезпечуючи платформу для складних кампаній впливу, які проводяться національними державами (Іран та інші), різними хакерськими групами, щоб донести своє повідомлення та рекламувати свої послуги, а зловмисники прагнуть обдурити інших користувачів розлучитися з конфіденційною інформацією або криптовалютою.

Фішери видають себе за великі британські банки у Twitter. Клієнти банків Великої Британії стають мішенню фішерів, які видають себе за обліковий запис служби підтримки клієнтів банків у Twitter (*Less than 20% of IT pros have complete access to critical data in public clouds, 2019*). Фішери вибирають варіанти назви законних облікових записів і повторюють їх зовнішній вигляд, а також вводяться, коли користувач ставить запитання до законного облікового запису. Для прикладу: підроблений обліковий запис – @BarclaysUKHelp, законний – @BarclaysHelpUK.

Фішер, що комплектує підроблений рахунок, відповідає та направляє користувача на фішинг-сайт, який дуже нагадує власну сторінку входу банку. Користувачі, які вводять свої

облікові дані в Інтернет-банкінгу на цей підроблений сайт, фактично передають свої дані шахраям. Іноді шахрайство не закінчується, і жертв просять ввести додаткову особисту та фінансову інформацію. Пізніше ця інформація буде використовуватися шахраями для обходу заходів безпеки банків та доступу до рахунку жертв.

Користувачам часто кажуть, що слід остерігатися небажаних повідомлень. Цей метод фішингу є високоефективним, оскільки користувач вже очікує відповіді від акаунта банку в Twitter і просто припускає, що отримане повідомлення надходить від банку. Звичайно, фішери роблять все можливе, щоб не викликати жодних підозр. Фішери використовують Twitter, щоб видавати себе за кожен великий банк Великої Британії. Раніше подібні атаки застосовувалися до користувачів PayPal. За даними компанії, фішинг у соціальних мережах зріс більш ніж на 100% у 2-3 кварталах 2020 року.

Офіційні облікові записи часто мають біля свого імені синю позначку «галочка». Якщо ні, виконайте короткий пошук у Twitter, щоб побачити, чи з'являються інші облікові записи, і якщо вони з'являються, уважно оцініть кожен із них та відсійте підробки.

Єдина платформа для захисту цифрових та соціальних каналів це платформа SaaS Cyber SafeGuard із широким охопленням каналів (соціальні медіа, мобільні додатки, мережі співпраці, магазини додатків тощо), вдосконаленими алгоритмами штучного інтелекту та машинним навчанням була розроблена для виявлення загроз у всіх цифрових каналах, що належать організації та захищатися від них.

За допомогою цієї платформи можливо поставити на карантин шкідливе програмне забезпечення, спам та фішинг, які мають місце у цифрових та соціальних облікових записах і використовуються для отримання доступу до організації. Надається можливість захистити облікові записи від злому облікових даних. Але, найголовніше, платформа адаптована до нових ризиків.

Шукаючи рішення для мінімізації ризиків у соціальних мережах, організації повинні пам'ятати про конфіденційність працівників.

Існують технології, політика та рішення для моніторингу, які можуть допомогти захистити від соціальних та цифрових ризиків, але жодна з них не є всеосяжною, деякі неефективні, а деякі не можуть масштабуватися – вони просто не можуть обробити всю інформацію та робочий процес усіх соціальних і цифрових каналів, які належать організації та не можуть негайно вживати заходів для придушення кожного ризику згідно із заздалегідь налаштованими правилами.

Хакерські атаки відбуваються в режимі реального часу, тому їх необхідно зупиняти у режимі реального часу (*How do you protect digital channels from cyber threats?, 2018*). Найбільша кількість шахрайських атак – у США та Китаї. Більше 21% фейкових акаунтів, націлених на онлайн та фінансові послуги, походять із США, а 17% – з Китаю. У атаках, націлених на північноамериканські онлайн-сервіси, більше 45% нападів було здійснено в США. Цікаво, що злочинні групи залучають різних постачальників хмарних послуг залежно від атаки. Шахраї, націлені на соціальні платформи, значною мірою використовують веб-служби Amazon, тоді як шахраям, націленим на мобільні додатки та фінансові послуги, віддають перевагу DigitalOcean.

Скоординовані атаки відбуваються групою шахрайських облікових записів, контрольованих одним і тим зловмисником представляють більшість шахрайських дій як у соціальних платформах, так і у фінансових службах (*Рис. 5*).

Більше 90% реєстрації фейкових акаунтів у соціальних платформах пов'язані з скоординованими атаками, у фінансовому секторі більше 40% шахрайства з додатками походить від скоординованих атак.

Хоча більшість шахрайських атак трапляється менше ніж через день після створення облікових записів, деякі акаунти "спальних клітин" можуть чекати місяцями або роками, перш ніж їх використовувати. В середньому шахрайські акаунти інкубуються 35 днів перед атакою (*For some cloud services more than 75% of accounts are utilized by hackers, 2018*).

Кожен хмарний сервіс має власний набір інструментів, дозволів, формату журналу та інтерфейсу, що робить безпеку новою проблемою для кожної програми. Важливо звернути увагу на відмінності між хмарними сервісами та вибрати правильний, виходячи з ваших потреб. Переконайтеся, що ви завжди можете сказати, хто і з якої причини отримує доступ до ваших конфіденційних даних, і що кожен доступ надходить із законного джерела.

Кібершахрайство

В останні роки, світовий ринок хмарних послуг має тенденцію щодо динамічного зростання на 20%. За прогнозними даними, у 2022 році IT-послуги можуть скласти близько $331 млрд, а відповідно світові витрати на публічні хмарні сервіси зростуть до 2023 року до $500 млрд.

Зростання кількості транснаціональних корпорацій щодо переміщення даних у публічні хмари відповідає актуальним питанням сьогодення. Найпопулярнішим світовим трендом є застосування глобальних публічних хмар, таких як Google Cloud, Microsoft Azure, Amazon Web Services.

З лютого 2022 року супутниковий інтернет Starlink від компанії SpaceX Ілона Маска розширив зону покриття в Україні. Компанія SpaceX встановила вже понад тисячу супутників для Starlink та продовжує розширювати покриття. Загалом SpaceX планує вивести на навколоземну орбіту 12 тис. таких супутників, а потім довести їх кількість до 30 тис.

Багато шахрайських облікових записів в банках видаляються через те, що виникає підозра щодо відмивання грошей та шахрайства. Цифрове суспільство не може безпечно існувати без надійної системи кібербезпеки. Щорічно відбувається дослідження рейтингу національного індексу кібербезпеки, який дає можливість вимірювати готовність країн запобігати кіберзагрозам і керувати ними.

За даними NCSI у 2021 році лідерами рівня національного індексу кібербезпеки у світі були: Греція, Литва, Бельгія, Чехія, Естонія, Німеччина, Португалія, Іспанія, Польща та Фінляндія (*Рис. 6*) (*Національний індекс кібербезпеки, 2020*). Україна у цьому рейтингу посіла 24 місце із показником 75,31. У рейтингу взяли участь 160 країн світу. Необхідно сказати, що рівень цифрового розвитку України становить 55,95, що є більше середнього в усьому світі.

Від кіберзлочинів, який є найпоширенішим із видів економічних злочинів, постраждало близько 31% організацій в Україні у 2021 році, які призвели до фінансових збитків та інших наслідків.

Близько третини українських організацій вказують, що постраждали від наслідків шкідливого програмного забезпечення, 38% українських респондентів зазначили, що їхні організації постраждали від вимагання через враження програмним забезпеченням типу ransomware. Майже кожна третя українська компанія (31%) має відповідні програми захисту від кібератак. До основних видів економічних злочинів та шахрайства, від яких постраждали компанії внаслідок кібератак у 2021 році, належать: порушення бізнес-процесів, вимагання, порушення прав інтелектуальної власності, атаки з політичним мотивом, незаконне привласнення майна, інсайдерська торгівля, шахрайство у сфері закупівель та інші (*Рис. 7*).

Найбільше компанії постраждали від кібератаки, в якій було застосовано шкідливе програмне забезпечення. Таких компаній в Україні 35%, а у світі 36% (*Рис. 8*). Від атак фішингу – в Україні постраждали 13% компаній, у світі майже у три рази більше 33%. Далі йдуть сканування мережі, атака методом підбору паролю, атака посередника. Необхідно зауважити увагу на такому важливому моменті, що більшість компаній не хочуть говорити про такі загрози, бо це впливає на імідж компаній, їх конкурентоспроможність та іноземних інвесторів, з якими вони працюють.

Застосування сучасних технологій для забезпечення постійного захисту та моніторингу для протидії економічним злочинам та шахрайству дозволяє 49% українським компаніям створювати захист своїх даних, а 51% компаній вказують, що застосування таких технології дає інформацію для вживання заходів щодо протидії економічним злочинам.

До технологій, які використовуються для протидії економічним злочинам або шахрайству належать: регуляторна аналітика, перевірка контрактів з клієнтами, моніторинг комунікацій, постійний моніторинг, моніторинг електронної пошти та інші (*Табл. 1*).

Аналізуючи загрози, які сталися внаслідок кібератак, необхідно сказати і про наявність фахівців у компаніях для протидії кібератакам. У 2021 році 6% компаній бракувало відповідних фахівців, фахівці 6% компаній покладалися на захист із зовнішніх ресурсів, потрібність у фахівцях, які володіють такими технологіями становить 37%, необхідність пройти навчання та підвищити кваліфікацію для 47% компаній є актуальним питанням.

Нульова довіра

Архітектура нульової довіри базується на припущенні, що жодній службі, серверу, ролі чи клієнту у вашій мережі не можна довіряти. Завжди двічі перевіряйте запити на доступ до конфіденційних даних, застосовуйте багатофакторну аутентифікацію, відстежуйте зміни в поведінці та впроваджуйте модель принципу найменшого привілейованого. Якщо ви можете визначити, як повинен поводитися кожен користувач, і до яких даних він має доступ, ви знаєте, як відстежувати цих користувачів.

Користувачів API (Application Programming Interface – це набір способів і правил взаємодії та обміну даними між різними програмами) слід обмежити відповідно до

пристрою-виробника, а також відстежуючи їх моделі поведінки, а привілейовані API повинні обмежуватися для роботи лише з внутрішньої мережі компанії. Нарешті, користувачі повинні постійно проходити аутентифікацію за допомогою багатофакторної автентифікації (MFA – побудований із поєднання фізичних, логічних та біометричних методів перевірки) і та контролювати їх за допомогою антивірусного програмного забезпечення.

Висновки

Таким чином, витік облікових даних може статися де завгодно, від зламаного персонального комп'ютера до сервера баз даних. Тому на кожному кроці доступу до секретної інформації користувачеві потрібно авторизуватись. Якщо, наприклад, використовується зовнішня служба авторизації, і ця служба має надійний обліковий запис у веб-програмі, ця веб-програма повинна забезпечити, щоб надійний обліковий запис використовувався службою, а не людиною посередині. Коли веб-сервер запитує доступ до секретної інформації, він повинен надходити із законного потоку, а не лише від когось із оболонкою на машині. Раптова зміна кількості підключених пристроїв або використання виклику API може свідчити про компроміс облікових даних.

Паролі використовуються на різних рівнях, від операційних систем до програм, а також інфраструктури. Багато користувачів записують пароль на бумазі, в блокнотах, в закладках та зберігають біля комп'ютера. Всім відомо як дратує постійне введення паролю. І ми ще деякий час матимемо паролі, але з часом ми будемо використовувати їх менше. Ми все ще матимемо їх у фоновому режимі, і вони, ймовірно, використовуватимуться як резервний метод. Але технологія безпарольного входу, яка підтримує автентифікацію на основі сертифікатів та забезпечує безпечне зберігання та керування сертифікатами, які прив'язані до користувача та конкретного пристрою, все більше завойовує простір. З точки зору безпеки, безпарольна реалізація на основі сертифікатів є набагато безпечнішою, ніж використання стандартних облікових даних. З точки зору конфіденційності, дані будуть більш захищеними, і оскільки все більше програм підтримує безпарольну технологію, буде важче отримати доступ до облікових записів користувачів, що впливатиме на безпеку персональних даних.



Список джерел інформації:

Вишня, В.Б. Гавриш, О.С., Рижков, Е.В. (2020). *Основи інформаційної безпеки: навч. посіб.* Дніпро: ДДУВС.

Гребенюк, А.М. та Рибальченко, Л.В. (2020). *Основи управління інформаційною безпекою: навч. посіб.* Дніпро: ДДУВС.

Національний індекс кібербезпеки (2020, September 30). Фонд електронного урядування Естонії. Отримано 27 березня 2022 року за https://ncsi.ega.ee/ncsi-index/?order=-rank

Рибальченко, Л.В. Рижков, Е.В. та Косиченко, О.О. (2019). Вплив тіньової економіки на економічну безпеку України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*, *2*, 175-183.

For some cloud services more than 75% of accounts are utilized by hackers (2018, October 20). Retrieved March 15, 2022 from https://www.helpnetsecurity.com/2018/10/04/cloud-based-online-user-accounts/ (англійс.)

Global Cybersecurity Outlook 2022. INSIGHT REPORT JANUARY 2022 (2022, January 30). The World Economic Forum. Retrieved March 15, 2022 from https://weforum.org (англійс.)

How do you protect digital channels from cyber threats? (2018, September 20) Retrieved March 15, 2022 from https://www.helpnetsecurity.com/2018/09/20/protect-digital-channels/ (англійс.)

Less than 20% of IT pros have complete access to critical data in public clouds (2019, March 26). Retrieved March 15, 2022 from https://www.helpnetsecurity.com/2019/03/26/access-critical-data-public-clouds/ (англійс.)

Rybalchenko, L., & Kosychenko, O. (2019). Features of latency of economic crimes in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. *Special Issue*, *1*, 264-267. (англійс.)

Rybalchenko, L., & Ryzhkov, E. (2019). Ensuring enterprise economic security. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. *Special Issue*, *1*, 268-271. (англійс.)

Rybalchenko, L., Ryzhkov, E., & Ohrimenco, S. (2021a). Modeling economic component of national security. *Philosophy, Economics and Law Review*, *1*(1), 25-36. (англійс.)

Rybalchenko, L., Ryzhkov, E., & Ohrimenco, S. (2021b). Economic crime and its impact on the security of the state. *Philosophy, Economics and Law Review*, *1*(2), 67-80. (англійс.)



Додаток

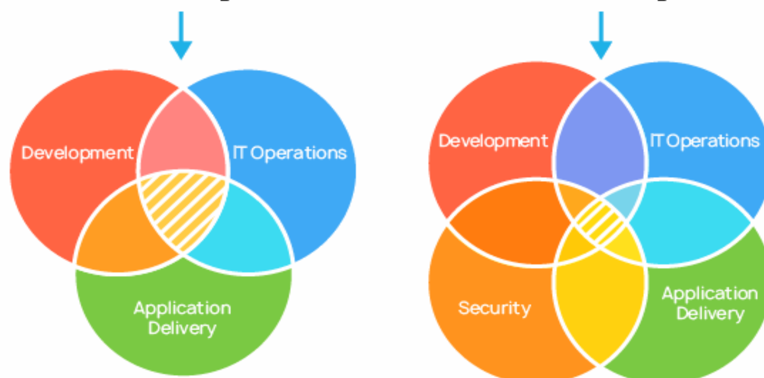


Рисунок 1. Відмінність DevOps та DevSecOps

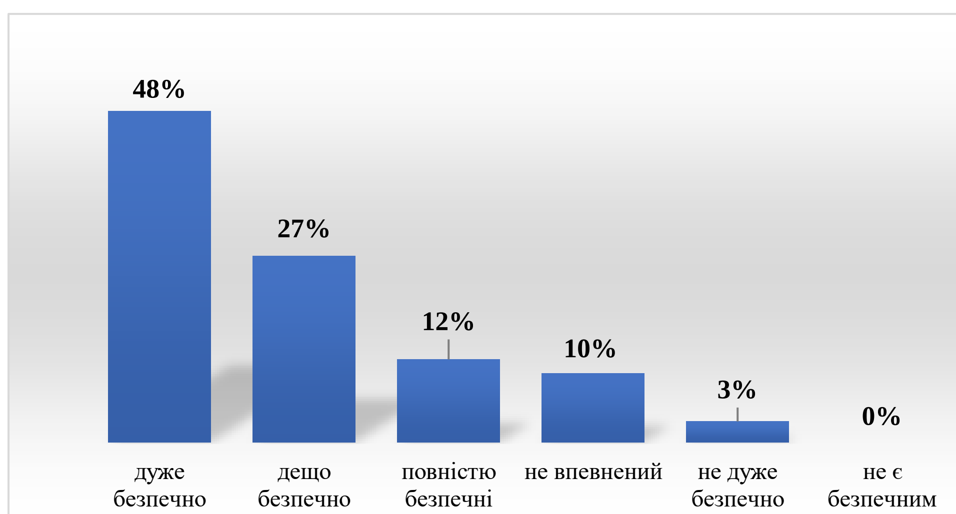


Рисунок 2. Наскільки безпечні безсерверні комп'ютери

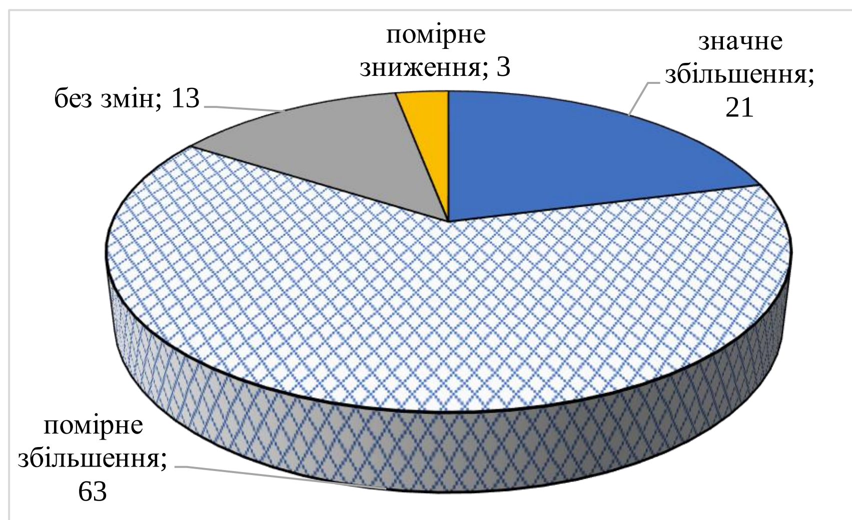


Рисунок 3. Збільшення обсягів роботи в хмарі, (%)

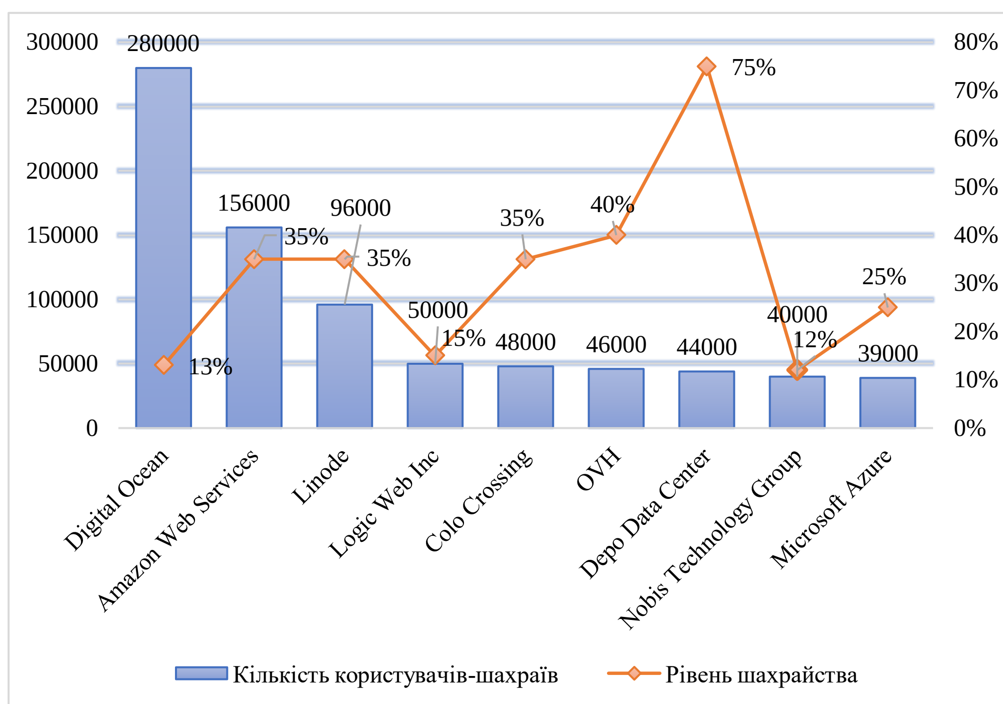


Рисунок 4. Найпопулярніші послуги хмарного хостингу з найбільшою кількістю шахрайських облікових записів

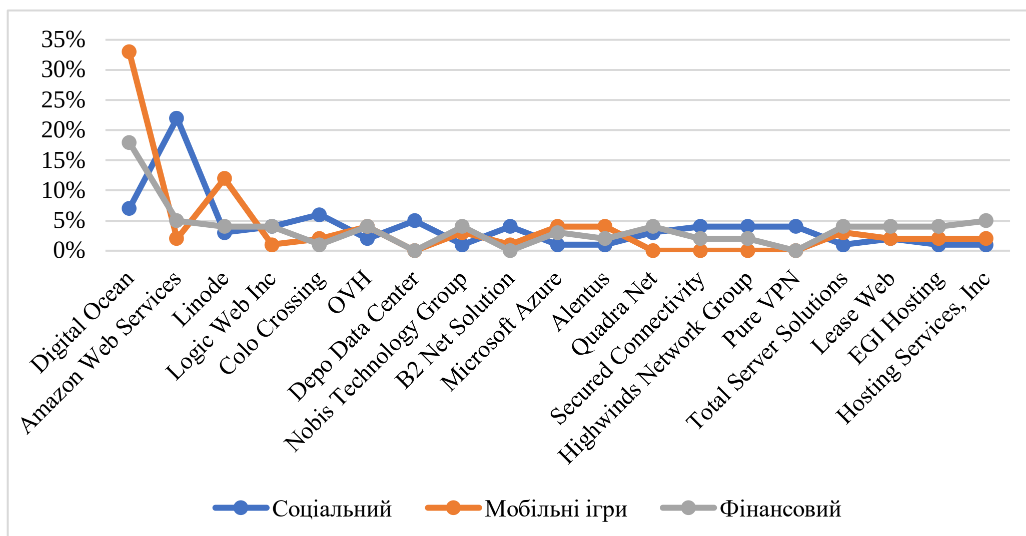


Рисунок 5. Частка шахрайських облікових записів, які походять із хмарних IP-адрес

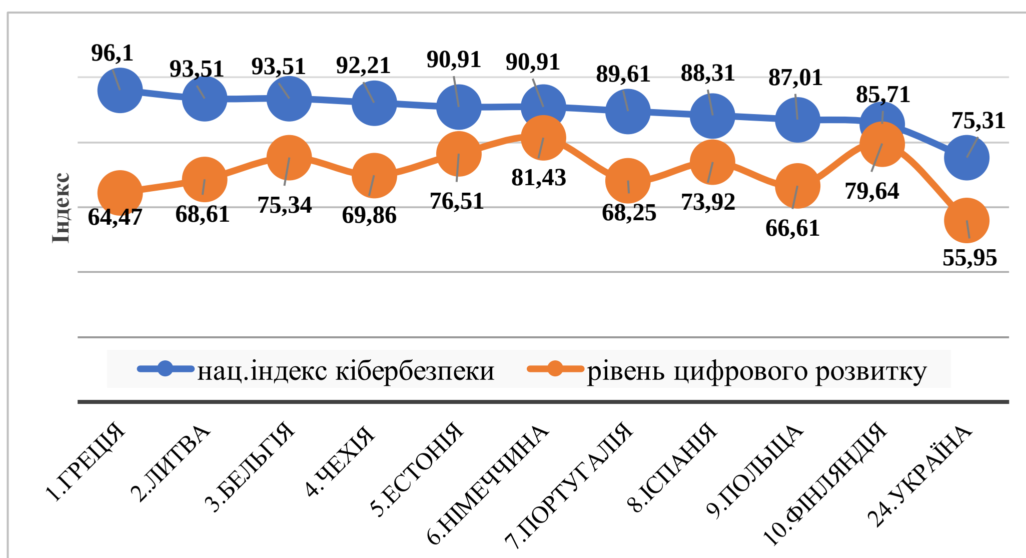


Рисунок 6. Топ-10 лідерів національного індексу кібербезпеки в країнах світу у 2021 році

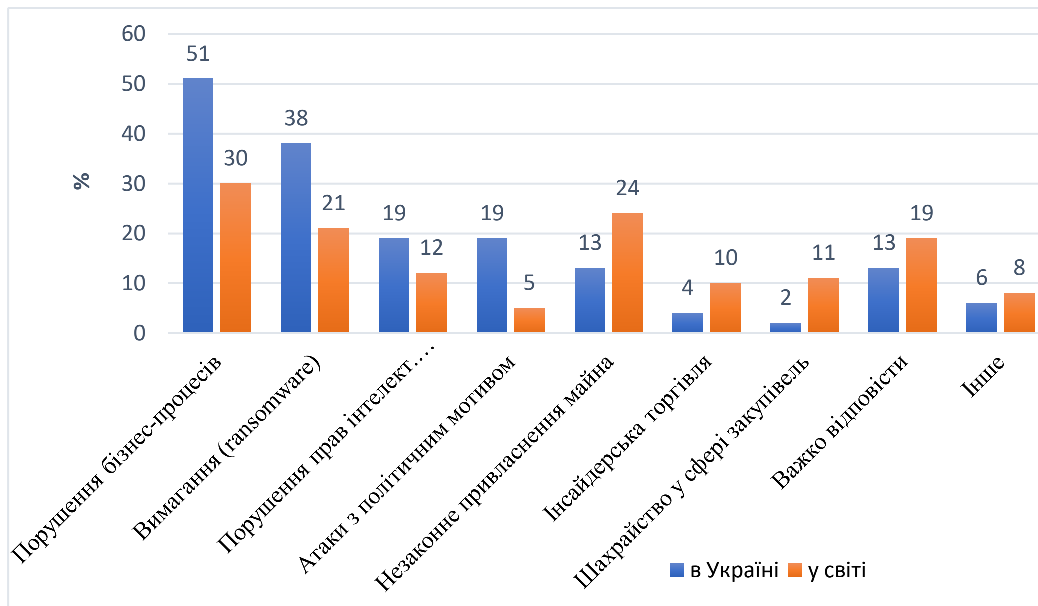


Рисунок 7. Види економічних злочинів та шахрайства, від яких постраждали компанії внаслідок кібератак у 2021 році

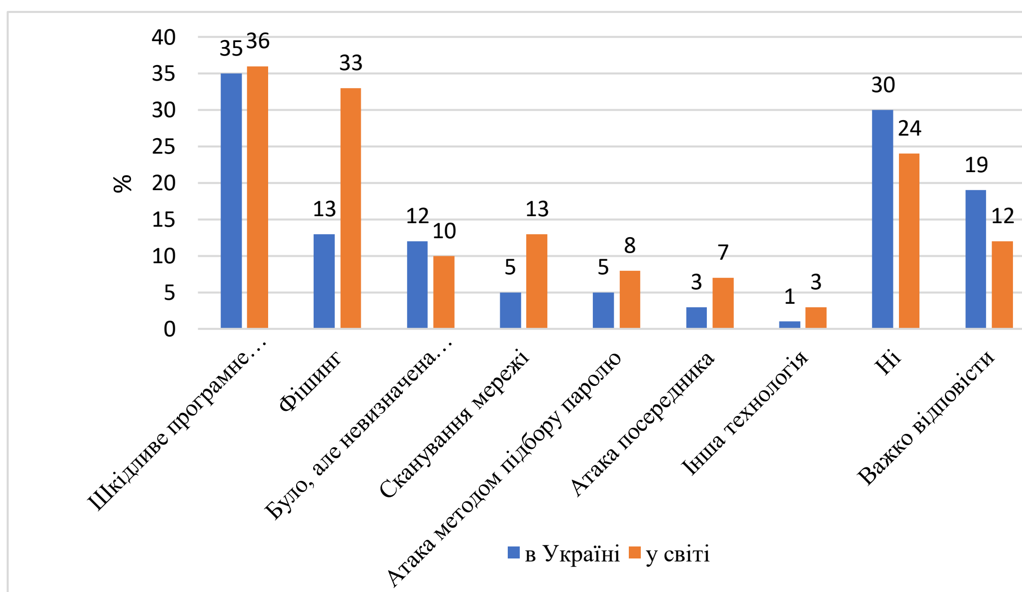


Рисунок 8. Компанії, які постраждали від кібератаки із застосуванням однієї із технологій

Таблиця 1. Використання сучасних технологій для протидії економічним злочинам або шахрайству

Технології	в Україні (%)	у світі (%)
Регуляторна аналітика	33	38
Перевірка контрактів з клієнтами	30	25
Моніторинг комунікацій	27	31
Постійний моніторинг	23	40
Тестування транзакцій	23	33
Практичне виявлення	22	31
Моніторинг електронної пошти	20	40
Обробка великих масивів даних	20	21
Залучення спеціалістів з аналізу даних	19	17
Виявлення схем поведінки	17	22
Моніторинг для управління ризиками	16	28
Візуалізація даних	13	28
Виявлення аномалій	13	30
Штучний інтелект	9	11